Contents

The prisoners and the n cube puzzle

- Cypher a number in an n-cube

I Abstract

We first present a few tools to solve " The prisoners and the n cube puzzle" which is described in chapter XV on page 25 , then we calculate solutions where they exist, and eventually give a few applications.

II The $\mathbb{F}_2$-vector space $\mathbb{F}_2^n$

Back to "Solving the puzzle": chapter XVI on page 25
Back to Case 4 chapter XIII on page 22

We denote $\mathbb{F}_2$ the field $\mathbb{Z}/(2)$, where (2) is the ideal of the $\mathbb{Z}$ ring generated by 2 ($\mathbb{F}_2 = \{0, 1\}$). For n integer, $\mathbb{F}_2^n$ (We define $\mathbb{F}_2^0 = \{0\}$), is the n times product of $\mathbb{F}_2$-vector space $\mathbb{F}_2$, by definition isomorphic to $\mathbb{F}_2[X]_{n-1}$ the polynomials of order equal or inferior to $n-1$ (for n strictly positive).

Let's consider the injection: $\mathbb{F}_2 \overset{\delta}{\hookrightarrow} \mathbb{Z}$, $\delta(0) \underset{\text{def.}}{=} 0$, $\delta(1) \underset{\text{def.}}{=} 1$, this yields an injection, δ^* from $\mathbb{F}_2[X]$ to $\mathbb{Z}[X]$:

$$s = \sum_I a_i X^i \in \mathbb{F}_2[X], \quad \delta^*(s) \underset{\text{def.}}{=} \sum_I \delta(a_i) X^i \in \mathbb{Z}[X] \quad I \subset \mathbb{N} \quad I \text{ finite}$$

Now considering:

$$\begin{array}{ccc} \mathbb{F}_2[X] & \longrightarrow & \mathbb{N} \\ s & \longmapsto & \delta^*(s)(2) \end{array}$$

this mapping is bijective [1] and we have the following scheme:

$$\begin{array}{lccccl} & & \mathbb{F}_2^n & \hookrightarrow & \mathbb{N} & \\ \text{so:} & & s & \sim & \delta^*(s)(2) & \text{(Count in base 2)} \\ \text{Example:} & \mathbb{F}_2^3 \ni (1,1,0) & & \sim & 1+2=3 & \end{array}$$

Remark: $|\mathbb{F}_2^n| = |\mathbb{F}_2|^n = 2^n$

III The G_n group

$I_n = [\![1, n]\!]$, n non zero integer, $e_i = (0, 0, \cdots, \underbrace{1}_{ith}, \cdots, 0) \in \mathbb{F}_2^n$ we set $I_o = \emptyset$

An affine space on $\mathbb{F}_2$ is isomorphic to a $\mathbb{F}_2$-vector space , we confound the two, and let β_i be the affine symmetry defined by:

$$\begin{array}{ccc} \mathbb{F}_2^n & \overset{\beta_i}{\longrightarrow} & \mathbb{F}_2^n \\ s & \longmapsto & \beta_i(s) = s + e_i \end{array}$$

Example: $\beta_2(0,1,1) = (0,1,1) + (0,1,0) = (0,0,1)$ Back to "Game strategy": chapter XVII on page 26

Let G_n be the abelian group generated by: $\mathbb{B}_n = \{\beta_1, \beta_2, \cdots, \beta_n\}$ we set $\mathbb{B}_o = \emptyset$

(G_n, o) is a free abelian group. [2]
We will denote: $G_o = \{1\}$, $\beta_o = 1$
Property: $\beta^2 = 1$ for every $\beta \in G_n$, 1 stands for identity.
Back to embedding proof in footnote 22 on page 9

1

Thanks to Euclidean division by iteration we can find $s \in \mathbb{F}_2[X]$ such that $\delta^*(s)(2) = n$ for any integer n, and this splitting is unique so that $\delta^*(s)$ is uniquely defined, since δ^* is injective, so is s.

2

We define $\prod_{\emptyset} \beta_i = 1$ (and $\sum_{\emptyset} e_i = 0$)

- commutativity: $\beta_i \beta_j = \beta_j \beta_i \quad i, j \in I_n$, straightforward,
- associativity: $\beta_i(\beta_j \beta_k) = (\beta_i \beta_j)\beta_k \quad i, j, k \in I_n$, straightforward,
- $1 \in G_n$, identity and for $i \in I_n \quad \beta_i^2 = 1 \Rightarrow \beta^2 = 1$ for any $\beta \in G_n$.

We have a handy homomorphism μ from G_n to $\mathbb{F}_2^n$: [3] Back to "n-cube": chapter V on the next page

$$\mu : \begin{array}{ccc} G_n & \xrightarrow{\mu} & \mathbb{F}_2^n \\ \prod_J \beta_i & \longmapsto & \mu\left(\prod_J \beta_i\right) \underset{\text{def.}}{=} \sum_J e_i \end{array}$$

Clearly μ is surjective, G_n contains at most $\sum_0^n \binom{n}{k} = 2^n$ elements, so $|G_n| = |\mathbb{F}_2^n|$, hence μ is injective, it is an isomorphism: $(G_n, \circ) \overset{\mu}{\sim} (\mathbb{F}_2^n, +)$ Back to "Game strategy": chapter XVII on page 26

Property: $\beta \in G_n \qquad \exists! I \in \mathscr{P}(I_n), \quad \beta = \prod_I \beta_i \sim \sum_I 2^{i-1}$ [4]
Back to "A distance on G_n": chapter VII on page 10

IV A G_n group action on $\mathbb{F}_2^n$

Back to "Solving the puzzle": chapter XVI on page 25 Back to "Preliminaries": chapter XVII on page 26
Back to "Strategy": chapter XVII on page 27

We define an action on $\mathbb{F}_2^n$ like this: $\beta \in G_n, s \in \mathbb{F}_2^n \qquad \beta.s \underset{\text{def.}}{=} s + \mu(\beta)$ [5]

Property: $\beta, \gamma \in G_n \qquad \beta.\mu(\gamma) = \mu(\beta) + \mu(\gamma) = \mu(\beta\gamma)$

This action is:

- transitive, there's only one orbit: $\mu(\gamma) \in \mathbb{F}_2^n, G_n.\mu(\gamma) = \mu(G_n\gamma) = \mu(G_n)$ [6]
- free (The stabilizer of any s in $\mathbb{F}_2^n$ is trivial): $\beta.s = s$ implies $\beta = 1$ for $s \in \mathbb{F}_2^n$ [7]

And so this action is simply transitive.

Eventually, the action of G_n upon $\mathbb{F}_2^n$ is isomorphic to group operation in G_n:

$$\beta \in G_n, s \in \mathbb{F}_2^n, \quad \beta.s \overset{\mu^{-1}}{\sim} \beta\mu^{-1}(s)$$

---

3 $I, J, K \subset I_n$, we use addition in $(\mathscr{P}(I_n), +)$ the boolean group
$\psi\left(\prod_J \beta_i \prod_K \beta_i\right) = \psi\left(\prod_{J+K} \beta_i\right) = \sum_{J+K} e_i$
$\psi\left(\prod_J \beta_i\right) + \psi\left(\prod_K \beta_i\right) = \sum_J e_i + \sum_K e_i = \sum_{J+K} e_i$

4 Let be $I, I' \in \mathscr{P}(I_n)$ such that $\beta = \prod_I \beta_i = \prod_{I'} \beta_i$, $\beta = \prod_{I+I'} \beta_i = 1$, $I + I' = \emptyset$, $I = I'$

5 This is actually an action:

- $\beta, \gamma \in G_n, s \in \mathbb{F}_2^n \quad (\beta\gamma).s = s + \mu(\beta\gamma) = s + \mu(\beta) + \mu(\gamma) = \beta.(s + \mu(\gamma)) = \beta.(\gamma.s)$
- $1.s = s + \mu(1) = s$

6 $g, \gamma \in G_n, g\gamma \in G_n, g\gamma\gamma \in G_n\gamma, g \in G_n\gamma, G_n \subset G_n\gamma, G_n = G_n\gamma$

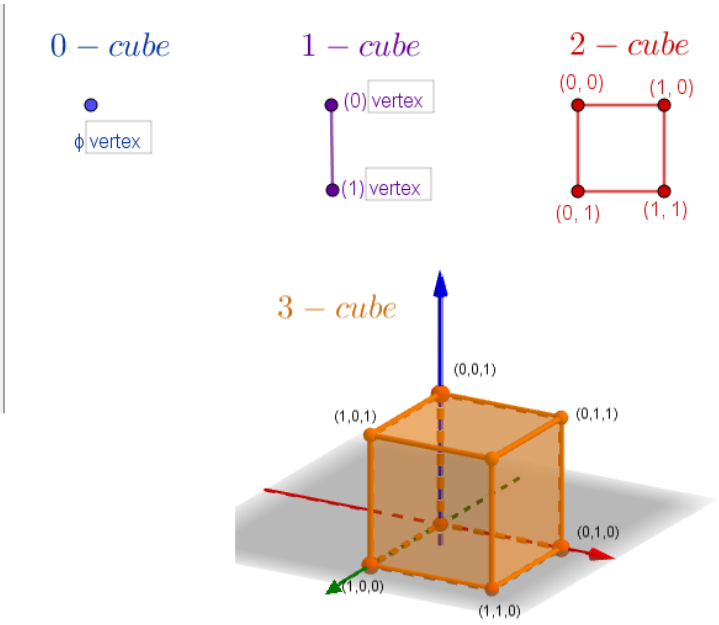
7 $\beta.s = s$, $s = s + \mu(\beta)$, $2s = 2s + \mu(\beta)$, $\mathrm{car}(\mathbb{F}_2) = 2$, $0 = \mu(\beta)$, $\beta = 1$

V The n-cube graph

We define the n-cube, as the graph whose vertices are $\mathbb{F}_2^n$ and edges:[8] $A_n = \{(s, \beta.s),\ s \in \mathbb{F}_2^n,\ \beta \in \mathbb{B}_n\}$.

Example: 0-cube is: $(\{O\}, \emptyset)$, $O = (0)$ (See figure: 1).
(The n-cube graph is an Eulerian graph.)

Figure 1: The n-cubes



VI The subgroups of G_n

We consider $(\mathscr{P}(G_n), +)$ the boolean group.
To simplify the script, for $\{\beta\} \in \mathscr{P}(G_n)$ we write simply β instead (Thus: $\{\beta_1, \beta_2\} = \beta_1 + \beta_2$, $\beta_1, \beta_2 \in G_n$).

Now we construct the product $\bullet$ in $\mathscr{P}(G_n)$.

$I, J \subset I_{2^n}$ $A = \sum_I a_i \in \mathscr{P}(G_n)$, $B = \sum_J a_i \in \mathscr{P}(G_n)$, $a_i \in G_n$

$$A \bullet B \underset{\text{def.}}{=} \sum_{IxJ} a_i a_j$$

---

8 Let's consider the affine space $O + \mathbb{F}_2^n$ on field $\mathbb{F}_2$. Since it is isomorphic to $\mathbb{F}_2^n$, we denote it: $\mathbb{F}_2^n$. $O = (0, \cdots, 0) \in \mathbb{F}_2^n$.

$\mathbb{F}_2 = \beta_1(O) + \{O\} = (1 + \beta_1) \bullet \{O\}$ $A_1 = \{(\{O\}, \beta_1(O))\}$ For a definition of operation "•" see VI

$\mathbb{F}_2^2 = (\beta_2 + 1) \bullet \mathbb{F}_2$ $A_2 = \{(\{O\}, \beta_1(O)), (\{O\}, \beta_2(O)), (\beta_1(O), \beta_2\beta_1(O)), (\beta_2(O), \beta_1\beta_2(O))\}$
$\mathbb{F}_2^n = \prod_{I_n} (1 + \beta_i)\{O\} = G_n \bullet \{O\}$

We stretch $\mathbb{F}_2^n$ in the $n+1$ dimension by means of the translation β_{n+1} and add it up to $\mathbb{F}_2^n \bullet \{O\}$ to obtain $\mathbb{F}_2^{n+1} \bullet \{O\}$.

So the n-cube graph is the affine space $\mathbb{F}_2^n \bullet \{O\}$ as vertices adjoined with the edges generated by the stretches at each step.

$\left(\mathscr{P}(G_n), \bullet\right)$ is a commutative monoid[9]

$\left(\mathscr{P}(G_n), \bullet, +\right)$ is a commutative ring[10]

Later on we will write AB instead of $A \bullet B$, whereby: $G_n = \prod_{I_n}(1+\beta_i) = \prod_{\mathbb{B}_n}(1+\beta)$ [11]

Automorphism on G_n

Example: $\sigma \in \mathscr{T}(I_n)$ the permutations of I_n, $I \in \mathscr{P}(I_n)$,

$$\varphi_\sigma : \begin{array}{ccc} G_n & \xrightarrow{\varphi_\sigma} & G_n \\ \prod_{i\in I}\beta_i & \longmapsto & \varphi_\sigma\left(\prod_I \beta_i\right) \underset{\text{def.}}{=} \prod_I \beta_{\sigma(i)} \end{array}$$

φ_σ is an automorphism[12].

Back to Proof: footnote 15 on the next page
Back to Example 2: chapter IX on page 14
Back to Property 2 footnote 53 on page 20

Let φ be an automorphism of G_n, H_1, H_2, two subgroups of G_n, direct product of G_n [13], then G_n is a direct product of $\varphi(H_1)$ and $\varphi(H_2)$: $G_n = \varphi(H_1)\varphi(H_2)$ [14]

9

- commutativity: G_n abelian
- identity: $I \subset I_{2^n}$, $A = \sum_I a_i \in \mathscr{P}(G_n)$, $A \bullet 1 = \sum_I a_i 1 = \sum_I a_i = A$, $1 \bullet A = A$
- associativity: $I, J, K \subset I_{2^n}$, $A = \sum_I a_i$, $B = \sum_J a_i$, $C = \sum_K a_i \in \mathscr{P}(G_n)$
  $A \bullet (B \bullet C) = \sum_I a_i \sum_{JxK} a_j a_k = \sum_{IxJxK} a_i a_j a_k = \sum_{IxJ} a_i a_j \sum_K a_k = (A \bullet B) \bullet C$

10

- $\left(\mathscr{P}(G_n), +\right)$ is an abelian group (The Boolean group) and,
- distributivity: $I, J, K \subset I_{2^n}$, $A = \sum_I a_i$, $B = \sum_J a_i$, $C = \sum_K a_i \in \mathscr{P}(G_n)$
  $A \bullet (B + C) = \sum_I a_i \sum_{J+K} a_j = \sum_{Ix(J+K)} a_i a_j \quad A \bullet B + A \bullet C = \sum_{IxJ} a_i a_j + \sum_{IxK} a_i a_k$
  for $j = k$ the sum $a_i a_j + a_i a_k = \emptyset$, $\quad A \bullet B + A \bullet C = \sum_{Ix(J+K)} a_i a_j$

11

Since $\prod_{\mathbb{B}_n}(1+\beta)$ contains $\sum_0^n \begin{pmatrix} n \\ k \end{pmatrix} = 2^n$ distinct elements.

12

$\prod_I \beta_i, \prod_J \beta_i \in G_n$, $I, J \in \mathscr{P}(I_n)$.
$\varphi_\sigma(\prod_I \beta_i)\varphi_\sigma(\prod_J \beta_i) = \prod_{I+J} \beta_{\sigma(i)} = \varphi_\sigma(\prod_{I+J} \beta_i) = \varphi_\sigma(\prod_I \beta_i \prod_J \beta_i)$

$\varphi_\sigma \varphi_{\sigma^{-1}} = \varphi_1 = 1$, 1=identity, so φ_σ is bijective.

13

that is: $G_n = H_1 H_2 = H_2 H_1$, $H_1 \cap H_2 = 1$ and for all $h_1 \in H_1$, $h_2 \in H_2$, $h_1 h_2 = h_2 h_1$

14

$s \in H_1$, $t \in H_2$, $\varphi(st) = \varphi(s)\varphi(t) \in \varphi(H_1)\varphi(H_2)$
$x \in \varphi(H_1) \cap \varphi(H_2) = \varphi(H_1 \cap H_2) = \varphi(1) = 1$, $x = 1$.

$G_{p+q} = HG_q$ with $H = \Pi_{i=q+1}^{p+q}(1+\beta_i)$, $\quad p, q \in I_n,\ p+q=n$

H is a subgroup of G_n isomorphic to G_p [15] and since $H \cap G_q = 1$, G_{p+q} is a direct product of G_q and H, henceforth:

G_{p+q} is isomorphic to G_pxG_q.

As a consequence:

- For any p in I_n, G_p is a subgroup of G_n, in particular $G_p \supset G_{p-1}$.
- $G_p \setminus G_{p-1} = \beta_p G_{p-1}$, $G_n = G_{n-1} + \beta_n G_{n-1}$
-

Any subgroup of G_n is isomorphic to a G_p group with $p \in I_n$ (1)

[16]

Back to subgroup G, chapter VI on page 8
Back to Proof, chapter VI on page 8
Back to "Back to case 3, footnote": chapter 55 on page 22

We denote: $< A >$ or $< \gamma_i >_I$ for $A \subset G_n$, $I \subset I_{2^n}$, $\gamma_i \in G_n$, the subgroup of G_n generated by $\{\gamma\}_A$, or respectively $\{\gamma_i\}_I$, thus:
$G_2 = < \beta_i >_{I_2} = < \beta_1 + \beta_2 >$, we will also write $< \beta_1, \beta_2 >$ instead.

Now let's consider the permutation[17] of G_n, Back to The isometry group : chapter IX on page 14

15
Via the isomorphism φ_σ of chapter VI on the preceding page , restricted to H: $H \mapsto G_p$, where: $\sigma(i) = i - q$ for $i \in I_n \setminus I_q$

16
Let H be a subgroup of G_n generated by $(\gamma_i)_{I_h}$, $I_h \subset I_{2^n}$, $\gamma_i \neq 1$ for $i \in I_h$, this family set being minimal for inclusion.

Let's prove first that $K, J \subset I_h$, if $\prod_J \gamma_i = \prod_K \gamma_i$ then $J = K$
Let be $K, J \subset I_h$, $J \neq K$, then $\prod_J \gamma_i \neq \prod_K \gamma_i$, otherwise $k \in K + J$, $\prod_J \gamma_i = \prod_K \gamma_i$ then $\prod_{(J+K)\setminus\{k\}} \gamma_i = \gamma_k$ and I_h would not be minimal.

Now consider:

$$\begin{array}{ccccc} & G_h & \xrightarrow{\varphi} & H \\ I \subset I_h & \prod_I \beta_i & \longmapsto & \prod_I \gamma_i \end{array}$$

φ is an isomorphism:

- φ is a morphism:
  $J, K \subset I_h$, $\quad \varphi\left(\prod_J \beta_i \prod_K \beta_i\right) = \varphi\left(\prod_{J+K} \beta_i\right) = \prod_{J+K} \gamma_i = \prod_J \gamma_i \prod_K \gamma_i = \varphi\left(\prod_J \beta_i\right)\varphi\left(\prod_K \beta_i\right)$
- φ is surjective by construction
- φ is injective:
  Let's assume that $\varphi\left(\prod_J \beta_i\right) = \varphi\left(\prod_K \beta_i\right)$ that is: $\prod_J \gamma_i = \prod_K \gamma_i$ from what precedes $K = J$, hence $\prod_J \beta_i = \prod_K \beta_i$

17 Since $\varphi_\gamma^2 = 1$ (The identity), φ_γ is bijective.

$\gamma \in G_n$:

$$\varphi_\gamma : \begin{array}{ccc} G_n & \xrightarrow{\varphi_\gamma} & G_n \\ s & \longmapsto & \gamma s \end{array}$$

Property: $\varphi_\gamma^2 = 1$ (The identity) Back to semidirect proof footnote 38 on page 15

And then $\mathscr{P}(G_n)$ has a natural structure of $\mathscr{P}(G_n)$-module on itself, the map:

$$\widetilde{\varphi_\gamma} : \begin{array}{ccc} \mathscr{P}(G_n) & \xrightarrow{\widetilde{\varphi_\gamma}} & \mathscr{P}(G_n) \\ A & \longmapsto & \varphi_\gamma(A) \end{array}$$

is $\mathscr{P}(G_n)$-linear[18]. Indeed:

· $\gamma \in G_n \quad A, B \in \mathscr{P}(G_n), \quad \varphi_\gamma(AB) = \varphi_\gamma(A)B$ [19]

In particular: $s \in G_n, \varphi(s) = s\varphi(1)$ Back to semidirect proof footnote 38 on page 15

Remark: For $A \subset G_n$ we denote: $\complement_A \underset{\text{def.}}{=} G_n \setminus A, \quad A, B \in \mathscr{P}(G_n), \gamma \in G_n, \gamma\complement_A = \complement_{\gamma A}, \gamma(A \cap B) = \gamma A \cap \gamma B, \gamma(A \cup B) = \gamma A \cup \gamma B$.[20]

Now consider the projection, P^p: $G_{p+q} \xrightarrow{P^p} G_p \text{x} 1$, we have $\ker P^p \sim G_q \quad \text{Im} P^p \sim G_p$ denoting π^p the canonical projection on G_{p+q}/G_q, there's a unique isomorphism $\widetilde{P}^p$ which renders the following commutative diagram:

$$\begin{array}{ccc} G_{p+q} & \xrightarrow{P^p} & G_p \text{x} 1 \\ \Big\downarrow{\scriptstyle \pi^p} & & \Big\uparrow{\scriptstyle \text{injection}} \\ G_{p+q}/G_q & \xrightarrow{\widetilde{P}^p} & G_p \end{array}$$

Back to Proof: footnote 32 on page 12

We also denote π_q the canonical projection on G_{p+q}/G_p corresponding to the projection P_q: $G_{p+q} \xrightarrow{P_q} 1 \text{x} G_q$.

Notations:
For (a, b) in $G_p \text{x} G_q$, we will denote $a \text{x} b$; for $(1, b)$, $1 \text{x} b$ or b.

---

[18] $A, B \in \mathscr{P}(G_n)$
· $\varphi_\gamma^2 = 1$, φ_γ bijective: $\varphi_\gamma(A + B) = \varphi_\gamma(A \setminus B \cup B \setminus A) = \varphi_\gamma(A) \setminus \varphi_\gamma(B) \cup \varphi_\gamma(B) \setminus \varphi_\gamma(A) = \varphi_\gamma(A) + \varphi_\gamma(B)$
· $\varphi_\gamma(AB) = \varphi_\gamma(A)B$: see footnote: 19

[19] $A = \sum_I a_i \quad B = \sum_J a_j \quad I, J \subset I_{2^n} \quad a_i \in G_n$
$\varphi_\gamma(\sum_{I \text{x} J} a_i a_j) = \sum_{I \text{x} J} \gamma a_i a_j = \varphi_\gamma(A)B$

[20] Since φ_γ permutation of G_n and $\varphi_\gamma(C) = \gamma C$ for any $C \in \mathscr{P}(G_n)$

$r \in G_n$ we will write: $r = s\text{x}t$, $s \in G_p$, $t \in G_q$.

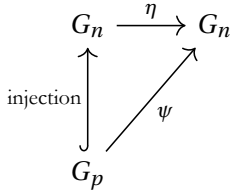
For $s\text{x}t \in G_p\text{x}G_q$ and $k \in I_n$ we will denote:
$\beta_k(s\text{x}t) = \beta_{k-q}s\text{x}t$ if $k \in I_n \setminus I_q$ and $\beta_k(s\text{x}t) = s\text{x}\beta_k t$ otherwise.

We will identify $\pi^p(G_n)$ and G_p or $G_p\text{x}1_q$ (1_q the neutral of G_q); $\pi_q(G_n)$ and G_q.
We will denote: π^0, π_0: $G_n \longrightarrow G_o = \{1\}$
In particular $A \in \mathscr{P}(G_n)$, $A = \pi^p(A)\text{x}\pi_q(A)$ that we will note: $A = \pi^p(A)\pi_q(A)$
Back to Property 1 footnote 51 on page 20 Back to calculus footnote 65 on page 28

Properties:

· Since π_q homomorphism, $a, b \in G_n$, $\pi_q(ab) = \pi_q(a)\pi_q(b)$ in particular $a\text{x}b \in G_p\text{x}G_q$, $\pi_q(a\text{x}b) = b$

Let G be a subgroup of G_n and ψ an isomorphism from G_p to G for a $p \in I_n$ well chosen (see proposition: 1 on page 6) .
We call η an automorphism of G_n, an embedding of G_n for ψ, if the restriction of η, to G_p equals to ψ that is: $\eta_{|G_p} = \psi$ with the following commutative diagram:



See examples in the footnote: [21] Back to proof in footnote: 38 on page 15

21

$G = 1 + \beta_1\beta_2\beta_3$, $G_2G = G_3$ (Since $|G_2G| = 2.4 = 2^3$, $GG_2 \subset G_3$, $G_2G = G_3$).

$\psi(1_2\text{x}G_1) = G$

η :

$$\begin{array}{ccccc} G_2 & \text{x} & G_1 & \overset{\eta}{\longrightarrow} & G_3 = G_2G \\ g & \text{x} & \beta_1 & \longmapsto & g\beta_1\beta_2\beta_3 \\ g & \text{x} & 1 & \longmapsto & g \end{array}$$

η is an isomorphism:
$g_1, g_2 \in G_2$
$\eta(g_1\beta_1\ g_2\beta_1) = \eta(g_1g_2) = g_1g_2 = \eta(g_1\beta_1)\eta(g_2\beta_1)$
$\eta(g_1\beta_1\ g_2) = g_1g_2\beta_1\beta_2\beta_3 = \eta(g_1\beta_1)\eta(g_2)$
$\eta(g_1g_2) = g_1g_2 = \eta(g_1)\eta(g_2)$

η has the announced property: by construction $\eta_{|1_2\text{x}G_1} = \psi$
Hereunder another example:

$G = 1 + \beta_1\beta_2$, $p = 1$

ψ	1	$\beta_1\beta_2$		
G_2	1	β_1	β_2	$\beta_1\beta_2$
η	1	$\beta_1\beta_2$	β_2	β_1

We have:

Property:

For any isomorphism ψ which sends G_p onto a subgroup G of G_n, we can construct an embedding η as above[22] and G_n is the direct product of G and G_q.

Back to Property 2 in footnote 55 on page 22
Back to General case, footnote: 59 on page 24
Back to General case, direct product footnote: 59 on page 24

$\eta(\beta_1\beta_2) = \beta_1$ $\quad$ $\eta(\beta_1)\eta(\beta_2) = \beta_1\beta_2\beta_2$
$\eta(\beta_1(\beta_1\beta_2)) = \beta_2$ $\quad$ $\eta(\beta_1)\eta(\beta_1\beta_2) = \beta_1\beta_2\beta_1$
$\eta(\beta_2(\beta_1\beta_2)) = \beta_1\beta_2$ $\quad$ $\eta(\beta_2)\eta(\beta_1\beta_2) = \beta_2\beta_1$

Thus η is an embedding of G_2 for ψ

22

G subgroup of G_n, we denote π_G the canonical projection onto G_n/G.
Let's choose a lift $\widetilde{\pi_G}$ of π_G such that $\widetilde{\pi_G}(1) = 1$. So we have: $\pi_G \circ \widetilde{\pi_G} = 1$
We denote $\overline{\gamma} = \gamma G$ the class of $\gamma \in G_n$

We posit: $\widetilde{\beta_i} = \widetilde{\pi_G}(\overline{\beta_i})$ for $i \in I_n$, then we define the map, ν: $G_n/G \longrightarrow G_n$ by: $\nu(\prod_I \overline{\beta_i}) = \prod_I (\widetilde{\beta_i})$, for $I \subset I_n$

- ν is a morphism:
  $\alpha = \prod_I \beta_i$, $\beta = \prod_J \beta_i$ $I, J \subset I_n$,
  $\nu(\overline{\alpha}\overline{\beta}) = \nu\left(\prod_{I+J} \overline{\beta_i}\right) = \prod_{I+J} \widetilde{\beta_i} = \prod_I \widetilde{\beta_i} \prod_J \widetilde{\beta_i}$, since for $i = j \in I_n$, $\widetilde{\beta_i}\widetilde{\beta_j} = \widetilde{\beta_i}^2 = 1$ see in chapter III on page 2 .

- $\pi_G \circ \nu = 1$:
  $\pi_G \circ \nu(\overline{\alpha}) = \pi_G \circ \nu\left(\prod_I \overline{\beta_i}\right) = \pi_G\left(\prod_I \widetilde{\pi_G}(\overline{\beta_i})\right) = \prod_I \pi_G \circ \widetilde{\pi_G}(\overline{\beta_i}) = \prod_I \overline{\beta_i} = \overline{\alpha}$.

Now consider the short exact sequence: $1 \longrightarrow G_p \xrightarrow{\psi} G_n \xrightarrow{\pi_G} G_n/G \longrightarrow 1$

where ψ is an isomorphism from G_p to G, $p \in I_n$.

ν is a split for the above sequence, so G_n is a semidirect product of G and G_n/G and G being abelian:
$G_n \sim G \times G_n/G$ then $1 \times G_n/G$ is a subgroup of G_n isomorphic to G_q since the index of G in G_n is q $(n = p + q)$ hence $G_n \sim G \times G_q$.
Now consider the map:

$$\varphi : \begin{array}{ccccc} G_p & \times & G_q & \xrightarrow{\psi \times 1} & G \times G_q \sim G_n \\ (s & \times & t) & \longmapsto & \psi(s) \times t \end{array}$$

It is a surjective morphism, so $\eta = \psi \times 1$ is an automorphism of G_n, which verifies: $\eta_{|G_p} = \psi$, it is an embedding of G_n for ψ.

Now having an embedding η of G_n for such an isomorphism ψ, then η passes to the quotient, by defining: $\overline{\eta}o\pi_q = \pi_G o\eta$ [23] with the following commutative diagram:

$$\begin{array}{ccc} G_n & \xrightarrow{\eta} & G_n \\ \downarrow{\scriptstyle \pi_q} & & \downarrow{\scriptstyle \pi_G} \\ G_n/G_p & \xrightarrow{\overline{\eta}} & G_n/G \end{array}$$

Back to Property 2 in footnote 55 on page 22 Back to case $n = 8$ in footnote 58 on page 23

$\overline{\eta}$ is an isomorphism[24]

VII A distance on G_n

Let be $s, t \in G_n$ we define the distance d_n on G_n by:

Let $J \subset I_n$ be the unique J (see Property in chapter III on page 3) such that $\prod_J \beta_i = st$,

$$d_n(s, t) \underset{\text{def.}}{=} |J|$$

[25]

We define: $\text{supp}\gamma \underset{\text{def.}}{=} J \in \mathscr{P}(I_n)$, the support of $\gamma = \prod_J \beta_i$

Back to Proof: footnote 51 on page 20

23

$\overline{\eta}$ is well defined:
$a, b \in G_n$ with $a = gb$, $g \in G_p$
We have: $\pi_G o\eta(a) = \pi_G o\eta(g)\pi_G o\eta(b) = \pi_G o\psi(g)\pi_G o\eta(b) = \pi_G o\eta(b)$
It is a morphism:
$a, b \in G_n$ with $a = \pi_q(a')$, $b = \pi_q(b')$
$\overline{\eta}(ab) = \pi_G o\eta(a'b') = \pi_G o\eta(a')\pi_G o\eta(b') = \overline{\eta}(a)\overline{\eta}(b)$

24

Since η bijection, $\pi_G o\eta = \overline{\eta}o\pi_q$ is surjective, $\overline{\eta}$ is surjective.

Now $|G_n/G| = |G_n/G_p|$, so $\overline{\eta}$ is a bijection.

25

- d_n is well defined, since G_n is a group and J unique.
- $d_n \in \mathbb{R}_+$ ($d_n \in [\![0, n]\!]$)
- for $s \in G_n$ $\quad d_n(s, s) = |\emptyset| = 0$
  $s, t \in G_n$ if $d_n(s, t) = 0$, $st = 1$ by definition, $s = t$
- d_n is symmetric since G_n is commutative
- $st = \prod_J \beta_i, \quad tr = \prod_K \beta_i \in G_n \rightsquigarrow sr = \prod_{J+K} \beta_i; \quad J, K \in I_n$
  $|J + K| \leq |J| + |K|$
  $d_n(s, r) \leq d_n(s, t) + d_n(t, r)$

Properties:
$m, r \in G_q \quad s, t, \sigma \in G_n$

- $d_n(s, t) = 1 \iff \exists \beta \in \mathbb{B}_n$ such that: $s = \beta t$
- $d_n(\sigma s, \sigma t) = d_n(s, t)$
- $d_n(\sigma s, t) = d_n(s, \sigma t)$
- $d_n(r, m) = d_q(r, m)$

Consequence: There's no triangle in G_n. [26]

We define: $s \in G_n, A \subset G_n \quad d_n(s, A) \underset{\text{def.}}{=} \min_{g \in A} d_n(s, g)$

We define for $\gamma \in G_n$: $\deg(\gamma) \underset{\text{def.}}{=} d_n(\gamma, 1)$, the degree of γ.

Properties:

- $s, t \in G_n, d_n(s, t) = d_n(st, 1) = \deg(st)$
- $\gamma \in G_n, \sigma \in \mathscr{I}(I_n), \deg(\varphi_\sigma(\gamma)) = \deg(\gamma)$ [27]

Back to σ_n^p properties footnote VIII on page 13
Back to semidirect proof footnote 38 on page 15

- $\alpha, \gamma \in G_n, \deg(\alpha) \neq \deg(\gamma) \Longrightarrow \alpha \neq \gamma$ [28]

Product distance

A, B being two metric spaces of distances d_A, d_B the product distance:
$d_{A \times B}(a \times b, c \times d) = d_A(a,c) + d_B(b, d) \quad a, c \in A, b, d \in B$ on $A \times B$ is a distance[29].

---

[26] that is: there are no $s, t, r \in G_n$ distinct, with $d_n(s, t) = 1 \quad d_n(s, r) = 1 \quad d_n(r, t) = 1$. Proof:
Let be $s, t, r \in G_n$ with the property in question, $st = \beta \in \mathbb{B}_n$, $sr = \gamma \in \mathbb{B}_n$, then $stsr = tr = \beta\gamma \in \mathbb{B}_n$, but $|\text{supp}\beta\gamma| = 2$, absurd.

[27] $\deg(\gamma) = |\text{supp}\gamma|$, $\deg(\varphi_\sigma(\gamma)) = |\text{supp}\varphi_\sigma(\gamma)| = |\sigma(\text{supp}\gamma)| = |\text{supp}\gamma|$

[28] i.e. $\alpha = \gamma \Longrightarrow \deg(\alpha) = \deg(\gamma)$

[29]

- $d_{A \times B} \in \mathbb{R}_+$, $d_{A \times B}$ is symmetric
- $d_{A \times B}(c, c') = 0 \Rightarrow c = c' \quad c, c' \in A \times B$
  $d_{A \times B}(c, c) = 0 \quad c \in d_{A \times B}$
- $a, a', a'' \in A \quad b, b', b'' \in B$

$$\begin{aligned} d_{A \times B}(a \times b, a' \times b') &= d_A(a, a') + d_B(b, b') \\ &\leq d_A(a, a'') + d_A(a'', a') + d_B(b, b'') + d_B(b'', b') \\ &\leq d_{A \times B}(a \times b, a'' \times b'') + d_{A \times B}(a'' \times b'', a' \times b') \end{aligned}$$

So for $p, q \in I_n$ on $G_p \text{x} G_q$ we have the product distance that we denote $d_{p\text{x}q}$:

$s_1 \text{x} t_1,\ s_2 \text{x} t_2 \in G_p \text{x} G_q \quad d_{p\text{x}q}(s_1 \text{x} t_1,\ s_2 \text{x} t_2) = d_p(s_1,\ s_2) + d_q(t_1,\ t_2)$

This distance coincides with the one on G_{p+q}: [30]

$s,\ t \in G_{p+q}, \quad G_{p+q} \overset{\varphi}{\sim} G_p \text{x} G_q \quad d_{p+q}(s,\ t) = d_{p\text{x}q}(\varphi(s),\ \varphi(t))$

Hence φ is an isometry. (see definition in chapter IX on page 14)
So we will write $d_{p+q}(s_1 \text{x} t_1,\ s_2 \text{x} t_2) = d_p(s_1,\ s_2) + d_q(t_1,\ t_2)$

This distance passes to the quotient.

Quotient distance $\tilde{d}^p$: $s,\ t \in G_n \quad \tilde{d}^p(\pi^p(s), \pi^p(t)) \underset{\text{def.}}{=} \min_{g \in G_q} d_{p+q}(gs,\ t)$ [31]

nota: $\tilde{d}^p(\pi^p(s), \pi^p(t)) \underset{\text{def.}}{=} \min_{g_1,\ g_2 \in G_q} d_{p+q}(g_1 s,\ g_2 t)$ is equivalent.

property: $\tilde{d}^p(\pi^p(s), \pi^p(A)) = d_p\big(\tilde{P}^p \text{o} \pi^p(s),\ \tilde{P}^p \text{o} \pi^p(A)\big)$ for $s \in G_{p+q}$ and $A \subset G_{p+q}$ [32]

---

[30]

$G_{p+q} \overset{\varphi}{\sim} G_p \text{x} G_q \quad I \subset I_n \setminus I_q,\ J \subset I_q \quad s = \prod_I \beta_i \prod_J \beta_i.\ d_{p+q}(s,\ 1) = |I| + |J|$
σ injection : $I_{p+q} \setminus I_q \quad \mapsto I_p \quad \sigma(q+i) \underset{\text{def.}}{=} i$
$\varphi(s) = \prod_I \varphi(\beta_i) \prod_J \varphi(\beta_i) = \big(\prod_{\sigma(I)} \beta_{\sigma(i)} \text{x} 1\big)\big(\prod_J 1 \text{x} \beta_i\big) = \big(\prod_{\sigma(I)} \beta_{\sigma(i)}\big) \text{x} \big(\prod_J \beta_i\big)$
$d_{p\text{x}q}(\varphi(s),\ 1\text{x}1) = d_p\big(\prod_{\sigma(I)} \beta_{\sigma(i)},\ 1\big) + d_q\big(1,\ \prod_J \beta_i\big) = |\sigma(I)| + |J| = |I| + |J| = d_{p+q}(s,\ 1)$
Now : $s_i \in G_p,\ t_i \in G_q$, for $i = 1, 2$
$d_{p\text{x}q}\big((s_1 \text{x} t_1)(s_2 \text{x} t_2),\ 1\text{x}1\big) = d_{p\text{x}q}(s_1 s_2 \text{x} t_1 t_2,\ 1\text{x}1) = d_p(s_1 s_2,\ 1) + d_q(t_1 t_2,\ 1) = d_p(s_1,\ s_2) + d_q(t_1,\ t_2) = d_{p\text{x}q}(s_1 \text{x} t_1,\ s_2 \text{x} t_2)$
from above:
$d_{p\text{x}q}\big((s_1 \text{x} t_1)(s_2 \text{x} t_2),\ 1\text{x}1\big) = d_{p+q}\big(\varphi^{-1}\big((s_1 \text{x} t_1)(s_2 \text{x} t_2)\big),\ 1\big) = d_{p+q}\big(\varphi^{-1}(s_1 \text{x} t_1)\varphi^{-1}(s_2 \text{x} t_2)\big),\ 1\big) = d_{p+q}\big(\varphi^{-1}(s_1 \text{x} t_1),\ \varphi^{-1}(s_2 \text{x} t_2)\big)$
the end of proof.

[31]

quotient distance:

$\tilde{d}^p$ is a distance:

- It is well defined: it doesn't depend on the s and t chosen for the class $\pi^p(s)$ and $\pi^p(t)$.
- $\tilde{d}^p \in \mathbb{R}_+$
- for $s,\ t \in G_{p+q} \quad \tilde{d}^p(\pi^p(s),\ \pi^p(t)) = 0$, there exists $g \in G_q \quad d_{p+q}(gs,\ t) = 0$, $gs = t$ that is $\pi^p(s) = \pi^p(t)$
  $\tilde{d}^p(s,\ s) = \min_{g \in G_q} d_{p+q}(gs,\ s) = d_{p+q}(s\ ,s) = 0$
- $\tilde{d}^p$ is symmetric since d_{p+q} is.
- $g_1, g_2 \in G_q \quad s,\ t,\ r \in G_{p+q}$

$$\begin{aligned} d_{p+q}(g_1 s,\ g_2 t) &\leq d_{p+q}(g_1 s,\ r) + d_{p+q}(r,\ g_2 t) \\ \min_{g_1,\ g_2 \in G_q} d_{p+q}(g_1 s,\ g_2 t) &\leq \min_{g_1,\ g_2 \in G_q} \big(d_{p+q}(s,\ g_1 r) + d_{p+q}(r,\ g_2 t)\big) \\ &\leq \min_{g \in G_q} \big(d_{p+q}(s,\ gr)\big) + \min_{g \in G_q} \big(d_{p+q}(r,\ gt)\big) \end{aligned}$$

[32]

Proof:
$s \sim s_1 \text{x} s_2 \in G_p \text{x} G_q$
$t \sim t_1 \text{x} t_2 \in G_p \text{x} G_q,\ t \in A$

$$\begin{aligned} \min_{g \in G_q} d_{p+q}(s,\ gt) &= d_p(s_1,\ t_1) + \min_{g \in G_q} d_q(1,\ s_2 t_2 g) \\ &= d_p(s_1,\ t_1) \\ \tilde{d}^p(\pi^p(s), \pi^p(A)) &= \min_{t_1} d_p(s_1,\ t_1) \\ &= d_p\big(\tilde{P}^p \text{o} \pi^p(s),\ \tilde{P}^p \text{o} \pi^p(A)\big) \text{ see diagram in chapter VI on page 7} \end{aligned}$$

This distance corresponds to d_p on $G_p \sim G_{p+q}/G_q$, since according to property above:
$\widetilde{d}^p(\pi^p(s), \pi^p(t)) = d_p\big(\widetilde{P}^p \circ \pi(s),\ \widetilde{P}^p \circ \pi(t)\big) = d_p\big(P^p(s),\ P^p(t)\big)$

Similarly we denote $\widetilde{d}_q$ stemming from $\widetilde{P}_q$, with the same terminology.

More generally, having a subgroup G of G_n, and the canonical homomorphism projection:
π_G: $G_n \longrightarrow G_n/G$ (since G_n is abelian, G is normal), we pass the distance d_n to the quotient by defining:
$\widetilde{d}(\pi_G(a), \pi_G(b)) \underset{\text{def.}}{=} \min_{\gamma \in G} d_n(\gamma a, b)$ for $a, b \in G_n$, the proof is similar to the one in footnote 31 on the preceding page. Back to embedding chapter: VI on page 9

VIII A partition of G_n by degrees

Now let's have a look at the polynomial $P \in \mathscr{P}(G_n)[X]$, defined by: $P = \prod_{I_n}(X + \beta_p) = \sum_{p=0 \text{ to } n} \sigma^n_{n-p} X^p$.

Which then defines $\sigma^n_p \in \mathscr{P}(G_n)$ for $p = 0, \cdots, n$.

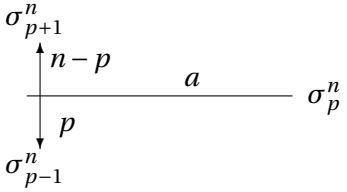
σ^n_p is the subset of the elements of G_n of degree p, $|\sigma^n_p| = \begin{pmatrix} n \\ p \end{pmatrix}$ and $\big(\sigma^n_p\big)_{p=0 \text{ to } n}$ is a (n+1)-partition of G_n, in particular $A \subset G_n \quad A = \sum_{p=0 \text{to} n} A \cap \sigma^n_p$. Back to proof in footnote: 38 on page 15

Example: for $n = 3$, $\sigma^3_3 = \beta_1\beta_2\beta_3$, $\sigma^3_1 = \beta_1 + \beta_2 + \beta_3$, $\sigma^n_o = 1$, $\sigma^n_1 = \mathbb{B}_n$

Definition: $a, b \in G_n$ are linked if $\deg(ab) = 1$

And so if $a, b \in G_n$ are linked, there exists $\beta \in \mathbb{B}_n$ such that $a = \beta b$. β is unique since G_n is a group, and we will call elements of $\mathbb{B}_n$, links. Back to proof in footnote: 38 on page 15
Properties 2:

- $a \in \sigma^n_p$, There are exactly $n - p$ elements of σ^n_{p+1}, and exactly p elements of σ^n_{p-1} linked to a. Those are the only links to a.[33] As a consequence: a belonging to σ^n_p is linked exactly to n elements and they all belong to σ^n_{p+1} or σ^n_{p-1}.(see the following diagram): Back to Proof: footnote 47 on page 19



- $\varphi_\sigma\big(\sigma^n_p\big) = \sigma^n_p \quad \sigma \in \mathscr{I}(I_n)$ [34]

33

$a = \prod_I \beta_i \in G_n$, with $I \in \mathscr{P}(I_n) \quad |I| = p$,
$b \in G_n$ with $\deg(ab) = 1$, $\quad b = a\beta_i$, $\quad$ either $i \in I_n \setminus I$ (occurrence: $|I_n \setminus I| = n - p$), $\deg b = p + 1$; $\quad$ or $i \in I$ (occurrence $|I| = p$), $\deg b = p - 1$

34

For $\gamma \in G_n$, $\deg\big(\varphi_\sigma(\gamma)\big) = \deg(\gamma)$ (see in chapter VII on page 11)

IX The isometric group $\mathscr{I}\text{som}$

Back to product distance: chapter VII on page 12

Let (G, d), (G', d') be metric groups ψ: $G \longrightarrow G'$, a bijective map. We say that ψ is an isometry, if:
$\forall_{G\times G'}(s, t) \quad d(s, t) = d'(\psi(s), \psi(t))$
We say that ψ is an isometry of G, when $G = G'$ Properties:

- The set of isometries of G_n altogether with the law of composition of mappings, is a group.[35]

We will call $\mathscr{I}\text{som}$ the set of isometries of G_n

Remark: Since $\mathscr{I}\text{som} \subset \mathscr{I}(G_n)$, the permutations of G_n, it is a finite group.

Example 1: φ_γ defined in chapter VI on page 6.
Example 2: φ_σ defined in chapter VI on page 5 is also an isometry.
Back to Property 2 footnote 53 on page 20

We denote:

- $G_\gamma = \{\varphi_\gamma \text{ for } \gamma \in G_n\}$
- $G_\sigma = \{\varphi_\sigma \text{ for } \sigma \in \mathscr{I}(I_n)\}$, $\mathscr{I}(I_n)$ the permutations of I_n

Properties:

- $\varphi \in \mathscr{I}\text{som}$ means that for any $(\alpha, \beta) \in G_n^2$, $\deg(\varphi(\alpha)\varphi(\beta)) = \deg(\alpha\beta)$
- G_γ is an abelian subgroup of the group $\mathscr{I}\text{som}$ isomorphic to G_n [36]
- G_σ is a subgroup of the group $\mathscr{I}\text{som}$ isomorphic to $\mathscr{I}(I_n)$ [37]

35

The set of bijective maps with the law in question is a group. φ, ψ, bijective maps, two isometries, for every t, s belonging to G_n, $d_n(\varphi\circ\psi(t), \varphi\circ\psi(s)) = d_n(\psi(s), \psi(t)) = d_n(s, t)$. So, the set of isometries is a sub-group of the bijective maps, thus a group.

36

Actually, G_γ is the image of G_n by the homomorphism :

$$\varphi : \begin{array}{ccc} G_n & \xrightarrow{\varphi} & \mathscr{I}\text{som} \\ \gamma & \longmapsto & \varphi_\gamma \end{array}$$

Back to Notations for elements of G_γ footnote IX on page 16
so it is a subgroup of $\mathscr{I}\text{som}$. Proof that φ is an homomorphism: $\alpha, \beta \in G_n \quad \varphi(\alpha\beta) = \varphi_{\alpha\beta} = \varphi_\alpha\circ\varphi_\beta = \varphi(\alpha)\circ\varphi(\beta)$
Also φ is injective since for $\varphi(\gamma) = 1$ (identity) in particular $\varphi_\gamma(1) = 1$ that is $\gamma = 1$ and then the image G_γ is isomorphic to G_n.
G_n being abelian, G_γ is also.

Nota:

$$\varphi^{-1} : \begin{array}{ccc} G_\gamma & \xrightarrow{\varphi^{-1}} & G_n \\ \varsigma & \longmapsto & \varsigma(1) \end{array}$$

37

G_σ is the image of $\mathscr{I}(I_n)$ by the homomorphism :

$$\xi : \begin{array}{ccc} \mathscr{I}(I_n) & \xrightarrow{\xi} & \mathscr{I}\text{som} \\ \sigma & \longmapsto & \varphi_\sigma \end{array}$$

- $\mathscr{I}\text{som}$ is the semidirect product of G_γ and G_σ, $\mathscr{I}\text{som} = G_\gamma \ltimes G_\sigma$ [38]
- the injective homomorphism:[39]

$$\varphi : \begin{array}{ccc} G_n & \xrightarrow{\varphi} & \mathscr{I}\big(\mathscr{P}(G_n)\big) \\ \gamma & \longmapsto & \varphi_\gamma \end{array}$$

Defines an action onto $\mathscr{P}(G_n)$:

$$\begin{array}{ccc} G_n \text{ x } \mathscr{P}(G_n) & \longrightarrow & \mathscr{P}(G_n) \\ (\gamma, \quad A) & \longmapsto & \gamma A = \varphi_\gamma(A) \end{array}$$

So it is a subgroup of $\mathscr{I}\text{som}$. Proof that ξ is an homomorphism: $\alpha, \beta \in \mathscr{I}(I_n) \quad \xi(\alpha \circ \beta) = \varphi_{\alpha\beta} = \varphi_\alpha \circ \varphi_\beta = \xi(\alpha) \circ \xi(\beta)$
Also ξ is injective since for $\xi(\sigma) = 1$ (identity) in particular $\varphi_\sigma(\beta_i) = \beta_i$ that is $\sigma(i) = i$ for all $i \in I_n$ and the image G_σ is isomorphic to $\mathscr{I}(I_n)$.

38

- $G_\sigma \cap G_\gamma = \{1\}$:
  $s \in G_n$, $\varphi \in G_\gamma \cap G_\sigma$, $\varphi(\varphi(1)) = \varphi^2(1) = 1$ according to VI on page 7, $\deg\big(\varphi(1)\big) = 0$ according to chapter VII on page 11, $\varphi(1) = 1$, $\varphi(s) = s\varphi(1) = s$, according to VI on page 7, $\varphi = 1$
- $\mathscr{I}\text{som} = G_\gamma \circ G_\sigma$:
  Let be $\varsigma \in \mathscr{I}\text{som}$, for $(\alpha, \beta) \in G_n^2$ we have: $\deg\big(\varsigma(\alpha)\varsigma(\beta)\big) = \deg(\alpha\beta)$, let's denote: $\varphi' \underset{\text{def.}}{=} \varphi\big(\varsigma(1)\big)$
  Because $\varphi' \circ \varsigma$ is an isometry we have also $\deg\big(\varphi' \circ \varsigma(\alpha)\varphi' \circ \varsigma(\beta)\big) = \deg(\alpha\beta)$. With $\beta = 1$, it comes: $\deg\big(\varphi' \circ \varsigma(\alpha)\big) = \deg(\alpha)$, since $\varphi' \circ \varsigma(1) = \varphi_{\varsigma(1)}\big(\varsigma(1)\big) = 1$

  $\varphi' \circ \varsigma$ leaves $\sigma_1^n = \mathbb{B}_n$ unchanged (And also any σ_n^p by the way), it is then a permutation of $\mathbb{B}_n$, so there exists $\sigma \in \mathscr{I}(I_n)$ such that: $\varphi_\sigma \circ \varphi' \circ \varsigma(\beta_i) = \beta_i$ for all $i \in I_n$, notice that $\varphi_\sigma \circ \varphi' \circ \varsigma(1) = 1$, remark also that since φ_σ leaves the degree unchanged $\varphi_\sigma \circ \varphi' \circ \varsigma$ also.

  Let's prove by induction on p that the restriction of $\psi \underset{\text{def.}}{=} \varphi_\sigma \circ \varphi' \circ \varsigma$ to σ_p^n is the identity:

  - For $p = 1$ that's true.
  - Assuming the property to be true up to $p \in I_n$, we have for any $I \subset I_n$ with $|I| = p + 1$, $i, j \in I$ $i \neq j$, denoting $\beta \in G_n$ whose $\text{supp}\beta = I$:

    $\psi(\beta)\beta\beta_i = \psi(\beta)\psi(\beta\beta_i)$ is of degree of β_i equal to 1, let's say that $\psi(\beta)\beta\beta_i = \beta_k$ for a $k \in I_n$, equally we have:
    $\psi(\beta)\beta\beta_j = \beta_{k'}$ for a $k' \in I_n$ which leads to:
    $\beta_i\beta_j = \beta_k\beta_{k'}$
    either $\beta_k = \beta_i$, $\beta_{k'} = \beta_j$, hence $\psi(\beta)\beta = 1$, $\psi(\beta) = \beta$
    or else $\beta_k = \beta_j$, $\beta_{k'} = \beta_i$, $\psi(\beta)\beta\beta_i = \beta_j$, $\psi(\beta) = \beta\beta_i\beta_j$, though $\psi(\beta)$ is of degree $p + 1$ and $\beta\beta_i\beta_j$ of degree $p - 1$ which is impossible. The end of the proof.

  So $\{\sigma_p^n\}_{p=0 \text{ to } n}$ being a partition of G_n (see in chapter VIII on page 13), $\varsigma = \varphi' \circ \varphi_{\sigma^{-1}}$, $\mathscr{I}\text{som} = G_\gamma \circ G_\sigma = G_\sigma \circ G_\gamma$

- G_γ is normal:
  $\sigma \in G_\sigma$, $\varsigma, \varsigma' \in G_\gamma$, $h \in G_n$, $(\sigma\varsigma')\varsigma(\varsigma'\sigma^{-1}) = \sigma\varsigma\sigma^{-1}$
  $\sigma\varsigma\sigma^{-1}(h) = \sigma\big(\sigma^{-1}(h)\varsigma(1)\big) = h\sigma\big(\varsigma(1)\big)$, $\sigma\varsigma\sigma^{-1} = \varphi\big(\sigma\varsigma(1)\big) \in G_\gamma$

39

- It is a homomorphism:
  $\gamma_1, \gamma_2 \in G_n$, $\varphi_{\gamma_1} \circ \varphi_{\gamma_2} = \varphi_{\gamma_1\gamma_2}$
- it is injective: $\mathscr{K}\text{er}\varphi \quad = \quad \{\gamma \in G_n, \varphi_\gamma = 1\}$
  $\varphi_\gamma \in \mathscr{K}\text{er}\varphi$, $\varphi_\gamma = 1$, in particular $1 = \varphi_\gamma(1) = \gamma$.

And so G_n acts faithfully on $\mathscr{P}(G_n)$ and for example we have:

$|G_n| = |\text{stabilizer}^n_A|.|\text{orbit}^n_A|_{\mathscr{P}(G_n)}$ for $A \in \mathscr{P}(G_n)$ [40]. That is the length of the orbit of A equals to the index in G_n of the stabilizer of A, in other terms: $\text{orbit}^n_A \sim G_n/G$, where $G \underset{\text{def.}}{=} \text{stabilizer}^n_A$

Nota: For $\gamma \in G_n$, and $A \in \mathscr{P}(G_n)$, we have, (group action) $\gamma A = \varphi_\gamma(A) = \gamma A$ (operation in the module $\mathscr{P}(G_n)$ on itself).

Notations:
Now for $\varsigma \in \mathscr{I}\text{som}$ we can also construct an action onto $\mathscr{P}(G_n)$ (definition: $\varsigma A = \varsigma(A)$), and so, in the following we will write: ςA instead of $\varsigma(A)$.

$A \in \mathscr{P}(G_n)$, G its stabilizer (see footnote: 40 for a definition), remarks:
Back to Property 2 in footnote 53 on page 20

- $GA = A \iff GA \subset A$
- If $1 \in A$, then $G \subset A$ [41] Back to proof on solution P_1 in footnote 54 on page 21

X The γ-core of G_n

Definition :
$A \in \mathscr{P}(G_n)$, $\gamma \in G_n$

- We say that A is a γ-core if it is stable by φ_γ (i.e. $\varphi_\gamma A \subset A$)
  If A is a γ-core, $\varphi_\gamma A = A \iff (1+\gamma)A = \emptyset$

XI The property P_o

Let P_o be the following property for a non empty set $A \in \mathscr{P}(G_n)$,

P_o : $\forall s \in G_n \quad d_n(A \setminus s, s) = 1$

In terms of n-cube $G_n \sim \mathbb{F}_2^n$ this means for any vertex s in $\mathbb{F}_2^n$ there exists an edge linking it to a vertex in A.

We will also later on use the weaker version of P_o:

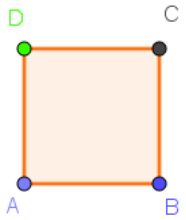
P_1: $\forall s \in G_n \quad d_n(A, s) \leq 1$

Example, see figure: 2 on the next page.

40
$\text{stabilizer}^n_A \underset{\text{def.}}{=} \{\gamma \in G_n / \ \gamma A = A\}$, it is a subgroup of G_n
$\text{orbit}^n_A \underset{\text{def.}}{=} \{B \in \mathscr{P}(G_n) / \ \exists \gamma \in G_n \quad B = \gamma A\}$
Back to remarks chapter IX

41
$1 \in A$ thus $G1 = G \subset A$

Figure 2: The properties P_o and P_1 for $n = 2$



$\{A, B\}$ with property P_o
$\{D\}$ without
$\{A, C\}$ with property P_1

Properties:

- $A \in \mathscr{P}(G_n)$ possesses the property P_o means that any element of G_n has a link to A.
- $A \in \mathscr{P}(G_n)$ possesses the property P_1 means that any element of $G_n \setminus A$ has a link to A.
- $P_o \Longrightarrow P_1$
- φ isometry, $A \in \mathscr{P}(G_n)$ satisfying P_o (respectively P_1), then φA satisfies P_o (respectively P_1), In particular: $G_{p+q} \overset{\varphi}{\sim} G_p \mathrm{x} G_q$, φA satisfies P_o (P_1)[42] Back to proof footnote 53 on page 20
- if $A \in \mathscr{P}(G_n)$ satisfying P_1 is a β_i-core $(i \in I_n)$ then A satisfies P_o[43]
  Back to Remarks footnote 51 on page 20 Back to Remarks footnote 53 on page 20
- $A \in \mathscr{P}(G_n)$ satisfying P_o, if $a \in A$ then $a \in \beta$-core for a $\beta \in \mathbb{B}_n$ [44]

42

- Case P_1: $\forall s \in G_n \quad d_n(A, \varphi^{-1} s) \leq 1,\ d_n(\varphi A, s) \leq 1$
- Case P_o: $\forall s \in G_n \quad d_n(A \setminus \varphi^{-1} s, \varphi^{-1} s) = 1,\ d_n(\varphi A \setminus s, s) = 1$

43

For $s \in A \quad \varphi_{\beta_i} s \in A$ and $d_n(s, \varphi_{\beta_i} s) = d_n(\beta_i, 1) = 1$ and in particular $\varphi_{\beta_i} s \in A \setminus s$

44

$a \in A$ has one link to A, so there is a $\beta \in \mathbb{B}_n$ such that $\beta a \in A$ that is $\varphi_\beta(a) \in A$

$A, B \subset G_n$ non empty subsets of G_n, A complying with P_1 then:

$$\text{If } B \supset A \text{ then } B \text{ satisfies } P_1 \tag{2}$$

[45] Back to Remarks chapter XII on the next page

$$\pi_q(A), \pi^p(A) \text{ comply with } P_1 \tag{3}$$

[46] Back to proof in footnote 51 on page 20

XII Some G_n partitions

Let k be a non null integer lower than $|G_n|$. We call a k-set of $\mathscr{P}(G_n)$, a disjoint set family of $\mathscr{P}(G_n)$ composed of k non empty subsets of G_n. We say that k is the size of the k-set.
We say that the k-set $(A_i)_{I_k}$ of $\mathscr{P}(G_n)$ is a partition if $\sum_{I_k} A_i = G_n$.

We say that $(A_i)_{I_k}$ a set family of $\mathscr{P}(G_n)$ " satisfies or complies with P_1" (respectively P_o) if it is a k-set of $\mathscr{P}(G_n)$ for which for each set A_i, P_1 (respectively P_o) holds.
We will call a set family which complies with P_1 (respectively P_o), a P_1-set (respectively a P_o-set), moreover if the corresponding k-set is a partition, we will name it a P_1-partition (respectively a P_o-partition), eventually we will call a P_o-core, a P_o-set whose elements are β-core for a $\beta \in \mathbb{B}_n$.

We denote hereunder: $\mathscr{A} = (A_i)_{I_k}$ a P_1-set of size k, with $k \geq 3$. The question is :

Does there exist such a set family of G_n ?

Such a set family if it exists, will be named a solution of size k for the problem P_1.

Remarks:

- A P_o-set is a P_1-set.
- $\varphi \in \mathscr{I}$som, if $\mathscr{A}$ is a P_o-set (respectively a P_1-set) then $\varphi\mathscr{A}$ is a P_o-set (respectively a P_1-set).
  Back to Property 2 footnote 53 on page 20

45

$\forall s \in G_n$, $d_n(A, s) \leq 1$ then a fortiori $d_n(B, s) \leq 1$

46

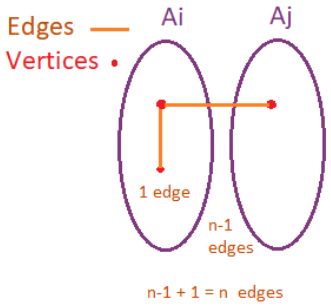
$\forall s \in G_n \quad \exists t \in A \quad d_{p\times q}(s, t) \leq 1$ a fortiori $\tilde{d}_q(\pi_q(s), \pi_q(t)) \leq 1$. $\pi_q(A) \neq \emptyset$. Idem for π^p.

- If $\mathscr{A}$ is a P_o-set then $k \leq n$ and if $k = n$ then $\mathscr{A}$ is an equipartition.[47]
  Back to proof P'_o footnote60 on page 25 Back to General case n footnote 59 on page 24
  Back to Theorem: chapter XIV on page 25
  And any element of $A \in \mathscr{A}$ belongs to a β-core whose cardinal is 2, for a $\beta \in \mathbb{B}_n$.[48]

- If $\mathscr{A}$ is a P_1-set then $k \leq n+1$ and if $k = n+1$ then $\mathscr{A}$ is an equipartition.[49]
  And any $A \in \mathscr{A}$ is β-core free for any $\beta \in \mathbb{B}_n$.[50]

- $\forall A_i \in \mathscr{A}$, for $A_j \in \mathscr{A}$, $j \neq i$, $A_j \subset \complement_{A_i}$ complies with P_1.

Figure 3: The case P_o



47

Since each element of G_n, has n links (see: VIII on page 13), this means that any element of A_i having already a link in A_i, has only $n-1$ links left to other A_j for $j \neq i$, henceforth $k-1 \leq n-1$ that is $k \leq n$.
If actually k does equal to n, since each element of A_i has only one link with an element of A_j, $j \neq i$; first there's no link left to reach out any element on $\complement_{\underset{In}{\cup} A_i}$, so $\complement_{\underset{In}{\cup} A_i} = \emptyset$ and $\mathscr{A}$ is a partition; second, A_i and A_j are in bijection since there is a link and only one link between two elements of them, so $\mathscr{A}$ is an equipartition (See figure: 3).

48

Since any element $a \in A \in \mathscr{A}$ has at least one internal link in A and at most one link in A to leave room for the links necessary towards the $n-1$ other members of the partition $\mathscr{A}$.

49

The proof is similar to the one above in footnote 42 , except for now we must have $k-1 \leq n$

50

Since any $\gamma \in G_n$ can't have an internal link in any $A_i \in \mathscr{A}$

Property 1:

If $\mathscr{A}$ is a solution of size n in G_{n-1} (i.e. a P_1-partition of size n in G_{n-1}), then[51]:

$$\left((1+\beta_n)A_i\right)_{I_n} \text{ is a } P_o\text{-core of } \mathscr{P}(G_n) \tag{4}$$

Back to case $n=8$ footnote 58 on page 23
Back to General case n footnote 59 on page 24

Property 2:

- If we have a solution $(A_i)_{I_{n+1}}$ in G_n (i.e. a P_1-partition of size $n+1$ in G_n) then we have a solution of the form $(\beta A)_{\beta\in 1+\mathbb{B}_n}$, $A\in\mathscr{P}(G_n)$, with $1\in A$[52]. We will call it a standard solution for G_n.
- If we have a P_o-partition of size n, then we have a P_o-partition of the form $(\beta A)_{\mathbb{B}_n}$, with 1, $\beta_n\in A$, $A\in\mathscr{P}(G_n)$. [53]

51

Proof:
Let $(B_i)_{I_k}$ be a P_1-set of $\mathscr{P}(G_q)$, p, q defined in chapter VI "The subgroups of G_n", $(k\le|G_q|)$.

- $G_p\text{x}B_i\cap G_p\text{x}B_j=G_p\text{x}(B_i\cap B_j)=\emptyset$ for $i,j\in I_k$, $i\neq j$
- $\underset{I_k}{\cup}(G_p\text{x}B_i)=G_p\text{x}\underset{I_k}{\cup}(B_i)\subset G_p\text{x}G_q\sim G_{p+q}$
- $G_p\text{x}B_i\sim\pi_q(B_i)$ hence $G_p\text{x}B_i$ satisfies P_1, see equation 3 on page 18
- $(1+\beta_n)(G_p\text{x}B_i)=(1+\beta_p)G_p\text{x}B_i=\emptyset$ (see in chapter VI on page 7), since $(1+\beta_p)^2=\emptyset$, hence $G_p\text{x}B_i$ is a β_n-core and thus P_o holds (see in chapter XI on page 17).

So, $(G_p\text{x}Bi)_{I_k}$ is a P_o-core of $\mathscr{P}(G_n)$

Applying this with $\mathscr{A}=(B_i)_{I_k}$, with $p=1$, $q=n-1$, $k=n$, completes the proof.

52

Let's suppose that we have a solution $\mathscr{A}=(A_i)_{I_{n+1}}$, and let's choose the only $A\in\mathscr{A}$ which contains 1 ($1\in A$).

Since A is β-core free for $\beta\in\mathbb{B}_n$, for $j\in I_n$ we have $\beta_jA\cap A=\emptyset$. Then if we have an element in $\beta_jA\cap\beta_kA$; $j\neq k$, $j,k\in I_n$ then there's a link from this element to two elements of A but this is impossible because an element of $G_n\setminus A$ can't have more than one link towards A: $\beta_jA\cap\beta_kA=\emptyset$. And so $(\beta A)_{1+\mathbb{B}_n}$ is a disjoint set family.
$\varphi_\beta A$ satisfies P_1, for $\beta\in\mathbb{B}_n+1$
$\sum_{1+\mathbb{B}_n}|\varphi_\beta A|=\sum_{1+\mathbb{B}_n}|A|=(n+1)|A|=|G_n|$. So $(\beta A)_{1+\mathbb{B}_n}$ is a solution.

53

Let's suppose that we have $\mathscr{A}$, a P_o-partition , and let's choose an $A\in\mathscr{A}$, such that $1\in A$, let a be an element in $\beta_iA\cap\beta_jA$, i, $j\in I_n$, $i\neq j$. So a has two links (β_i and β_j) towards A, whether a belongs to A or not this is impossible.

So $(\beta A)_{\mathbb{B}_n}$ is a disjoint family.
Now $|\sum_{\mathbb{B}_n}\varphi_\beta A|=\sum_{\mathbb{B}_n}|A|=n|A|=|G_n|$, hence $(\beta A)_{\mathbb{B}_n}$ is a P_o-partition (see in chapter XI on page 17).

we may assume that $\beta_n\in A$:
For an $i\in I_n$ well chosen $1\in\beta_iA$, thus $\varphi_{(i,\,n)}A$ contains 1 and β_n and $\left(\beta\varphi_{(i,\,n)}A\right)_{\mathbb{B}_n}$ is a P_o-partition since $\varphi_{(i,\,n)}$ is an automorphism and an isometry (see XII on page 18, IX on page 14).

Property 3:

- $(\beta A)_{\beta\in 1+\mathbb{B}_n}$, $A\in\mathscr{P}(G_n)$, a standard solution of size $n+1$, $n\geq 3$ then:

  $\sigma_1^n\cap A=\emptyset,\quad \sigma_2^n\cap A=\emptyset,\quad |\sigma_3^n\cap A|=\frac{|\sigma_2^n|}{3}$

  Consequence: For $n=3,\quad A=1+\sigma_3^3,\quad$ which is also the stabilizer of A [54]
  Back to case $n=4$ footnote 55 on the following page

54

Let $\mathscr{A}=(A\beta)_{\beta\in 1+\mathbb{B}_n}$ be a solution of size $n+1$, $A\in\mathscr{P}(G_n)$, $1\in A$.

$\beta_i,\beta_j\in 1+\mathbb{B}_n,\ \beta_i\neq\beta_j,\ \beta_i A\cap\beta_j A=\emptyset$

- for $i=0$ since $1\in A$ we get $A\cap\beta_j A=\emptyset\Longrightarrow\beta_j\notin A$ so $A\cap\sigma_1^n=\emptyset$
- for $i\neq 0$ and $j\neq 0$ we get $\emptyset=\varphi_{\beta_j}(\beta_i A\cap\beta_j A)=\beta_i\beta_j A\cap A\Longrightarrow\beta_i\beta_j\notin A$ so $A\cap\sigma_2^n=\emptyset$
- Each element of degree 3 in A generates exactly 3 elements of degree 2 in $\mathbb{C}_A$, necessarily different (and there are the whole lot of them since A has no element of degree 2). This means that $3|\sigma_3^n\cap A|=|\sigma_2^n|$
- If $n=3$, since then $|A|=\frac{|G_3|}{4}=2$ this clearly means that $A=1+\sigma_3^3$. Also the stabilizer of A which is included in A (see IX on page 16), is either A or 1, so it is A, because A is a group.

XIII The case P_o

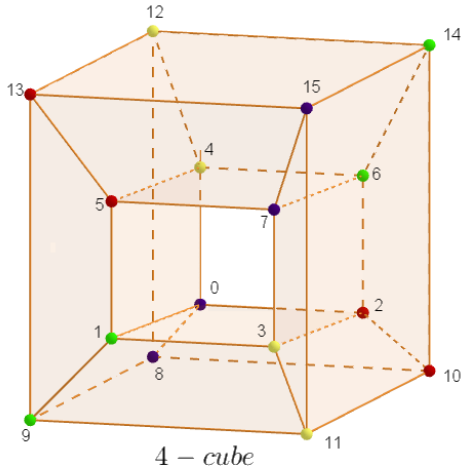
Back to "Solving the puzzle": chapter XVI on page 25

Case $n = 4$

Hereunder in rows the 4-partition of G_4 complying with P_o in question[55]. See figure 4:

$1 + \beta_1\beta_2\beta_3 + \beta_4 + \beta_1\beta_2\beta_3\beta_4 \sim \{0, 7, 8, 15\}$ see in chapter II on page 1
$\beta_1 + \beta_2\beta_3 + \beta_1\beta_4 + \beta_2\beta_3\beta_4 \sim \{1, 6, 9, 14\}$
$\beta_2 + \beta_1\beta_3 + \beta_2\beta_4 + \beta_1\beta_3\beta_4 \sim \{2, 5, 10, 13\}$
$\beta_3 + \beta_1\beta_2 + \beta_3\beta_4 + \beta_1\beta_2\beta_4 \sim \{4, 3, 12, 11\}$

Figure 4: A 4-cube P_o 4-partition



55

We look first for a 4-equipartition in G_3 which satisfies P_1 of the form $\mathscr{A} = (\beta G)_{\mathbb{B}_3+1}$, where $G = 1 + \sigma_3^3$ (see Property 3:XII on the preceding page).

Now let's consider orbit_G^3 with $G = 1 + \sigma_3^3$.
Since G is a group (thus isomorphic to G_1, see proposition 1 on page 6), and the stabilizer of G a subset of G (because $1 \in G$), the stabilizer of G, is G of index 2 in G_3. G_3 is the direct product of G and G_2 (see VI on page 9), and $\text{orbit}_G^3 \sim G_3/G \sim G_2$ whose elements are classes of[57] $1, \beta_1, \beta_2, \beta_1\beta_2 \overset{\sigma_3^3}{\sim} \beta_3$, $\sum_{\text{orbit}_G^3} A = \sum_{\mathbb{B}_3+1} \beta G = \sum_{G_2} \beta G$, and $(A)_{\text{orbit}_G^3}$ is an equipartition of G_3.

Note that for $\beta, \beta' \in \mathbb{B}_3 + 1$, necessarily $\beta\beta' G = \beta'' G$ with $\beta'' \in \mathbb{B}_3 + 1$ since it belongs to the orbit of G. Now let be $b \in G_3$, $b = \beta g$ with $\beta \in \mathbb{B}_3 + 1$ and $g \in G$: $d_3(b, \beta' G) = d_3(g, \beta'' G) \le d_3(g, \beta'' g) = d_3(1, \beta'') \le 1$, henceforth P_1 holds.
$(A)_{\text{orbit}_G^3}$ is a solution of size 4 in G_3 for P_1.

From property 1 equation 4 on page 20 we know then that $\left((1 + \beta_4)(1 + \sigma_3^3)\beta\right)_{\mathbb{B}_3+1}$ is a P_o-core.
Nota: $(1 + \beta_4)(1 + \sigma_3^3) = 1 + \beta_1\beta_2\beta_3 + \beta_4 + \beta_1\beta_2\beta_3\beta_4$

57

$\sum_{\mathbb{B}_3+1} \beta G \sim \sum_{\mathbb{B}_3+1} \pi_G(\beta) = \sum_{G_2} \pi_G \circ \eta(\beta) = \sum_{G_2} \overline{\eta} \circ \pi_2(\beta) = \overline{\eta}\left(\sum_{G_2} \pi_2(\beta)\right) \sim \sum_{G_2} \pi_2(\beta)$, see chapter VI on page 10

Note that $\left(\pi_G(\beta)\right)_{\mathbb{B}_3+1}$ holds P_1, whereas $\left(\pi_2(\beta)\right)_{G_2}$ doesn't, because neither η nor $\overline{\eta}$ are isometry.

Case $n = 8$

Hereunder a 8-partition of G_8 complying with P_o:

$$\left((1+\beta_8)\beta G\right)_{1+\mathbb{B}_7}$$ [58]

where G is the subgroup of G_8 of order $2^4 = 16$, generated by $\{\beta_1\beta_2\beta_4,\ \beta_2\beta_3\beta_5,\ \beta_1\beta_3\beta_6,\ \beta_1\beta_2\beta_3\beta_7\}$

58

We look first for a P_1-partition of size 8 in G_7, of the form $\sum_{1+\mathbb{B}_7} \beta G = \sum_{G_3} \beta G \sim \sum_{G_3} \beta G_4 \text{x} 1_3$, where G is a subgroup of G_7 of order $\frac{|G_7|}{8} = |G_4|$, as such the sum would be actually a partition, as the classes of the elements of G_3 in G_7 for π_3 (see VI on page 10, with $q = 3$).

The subgroup of G_7, $G = <\beta_1\beta_2\beta_4,\ \beta_2\beta_3\beta_5,\ \beta_1\beta_3\beta_6,\ \beta_1\beta_2\beta_3\beta_7>$ does the job, proof:
Back to "General case, subgroup G": footnote 59 on the following page
Back to "Game strategy": chapter XVII on page 26
Let's denote:
$g_4 = \beta_1\beta_2\beta_4, \quad g_5 = \beta_2\beta_3\beta_5, \quad g_6 = \beta_1\beta_3\beta_6, \quad g_7 = \beta_1\beta_2\beta_3\beta_7$

- About the first equality:

  For $\beta_i \in 1+\mathbb{B}_3$, $\beta_i \in G_3$

  $\beta_4 = \beta_1\beta_2 g_4$, $\beta_5 = \beta_2\beta_3 g_5$, $\beta_6 = \beta_1\beta_3 g_6$, $\beta_7 = \beta_1\beta_2\beta_3 g_7$

- G is actually a subgroup of G_n of order 2^4:
  We have $\pi^4(<\beta_1\beta_2\beta_4,\ \beta_2\beta_3\beta_5,\ \beta_1\beta_3\beta_6,\ \beta_1\beta_2\beta_3\beta_7>) = <\beta_4,\ \beta_5,\ \beta_6,\ \beta_7> \overset{\varphi}{\sim} G_4$ for a $\varphi \in G_\sigma$ well chosen,
  so $G \supset \left(\pi^4\right)^{-1}(\varphi G_4)$ is a subgroup of order greater than 2^4, and it contains at most 2^4 elements, so it is isomorphic to G_4

- The partition satisfies P_1:
  This means that $\forall_{G_3}\ \beta, \beta', \forall_G\ g \quad \left(d_7(\beta g, \beta' G) \le 1 \iff d_7(\beta\beta', G) \le 1\right)$, which is equivalent to: $\forall_{G_3}\ \beta \quad \exists_G\ g\ \deg(\beta g) \le 1$

  For $\beta \in 1+\mathbb{B}_3$ $\deg(\beta 1) \le 1$

  For $\beta \in G_3 \setminus \{1+\mathbb{B}_3\}$, by construction $\exists_{[\![4,\ 7]\!]}\ i \quad \beta\beta_i = g_i$, $\deg(\beta g_i) = \deg(\beta_i) = 1$, ok.

So $\mathscr{A} = (\beta G)_{G_3}$ is a solution of size 8 in G_7.
Now we know from property 1 (see equation 4 on page 20) that
$(1+\beta_8)\mathscr{A}$ is a P_o-core of G_8.

Find hereunder a complete description of G:

$$\begin{aligned}
G = \{&g_4, && g_5, && g_6, && g_7\\
&g_4g_5, && g_4g_6, && g_4g_7, &&\\
&g_5g_6, && g_5g_7, && g_6g_7, &&\\
&g_4g_5g_6g_7, && 1, &&&&\\
&g_5g_6g_7, && g_4g_6g_7, && g_4g_5g_7, && g_4g_5g_6\}\\
G = \{&\beta_1\beta_2\beta_4, && \beta_2\beta_3\beta_5, && \beta_1\beta_3\beta_6, && \beta_1\beta_2\beta_3\beta_7\\
&\beta_1\beta_3\beta_4\beta_5, && \beta_2\beta_3\beta_4\beta_6, && \beta_3\beta_4\beta_7, &&\\
&\beta_1\beta_2\beta_5\beta_6, && \beta_1\beta_5\beta_7, && \beta_2\beta_6\beta_7, &&\\
&\sigma_7^7, && 1, &&&&\\
&\beta_3\beta_5\beta_6\beta_7, && \beta_1\beta_4\beta_6\beta_7, && \beta_2\beta_4\beta_5\beta_7, && \beta_4\beta_5\beta_6\}
\end{aligned}$$

General case n, a power of two, a P_o-partition of G_n

Back to Theorem: chapter XIV on the next page

Hereunder a P_o-partition of G_n:

$$\left((1+\beta_n)\beta G\right)_{1+\mathbb{B}_{n-1}}$$ [59]

where G is a subgroup of G_{n-1} of index n, (see footnote 59 for a comprehensive description of this group) Back to "Solving the puzzle": chapter XVI on the next page

Miscellaneous

For $n=3$ there is no P_o-partition since it should be an equipartition (see XII on page 19) but the cardinal of G_3 is prime to 3. And for the case $n=2$, you'll find a P_o-partition in the fig. : 2 on page 17, namely: $\{A, B\}, \{D, C\}$. The case $n=1$ corresponding to the chessboard having only one tile is trivial, whereas the case $n=0$, corresponds to the chessboard having no tile (So an empty partition would have been suitable but it's not a P_o-set by definition).

59

Back to "Game strategy": chapter XVII on page 26

Since the P_o-partition in G_n if it exists, is an equipartition (see XII on page 19), n must be a power of 2, say: $n=2^h$, $h\in\mathbb{N}$.

Let σ be an injection from $[\![1, n-1-h]\!]$ to $G_h\setminus\{1+\sigma_1^h\}$

Let's define $\tilde{\psi}(i) \underset{\text{def.}}{=} \beta_i x \sigma_i$ for $i\in[\![1, n-1-h]\!]$

Now we have the injective group morphism:

$$I\subset I_{n-1-h},\quad \begin{array}{ccc} G_{n-1-h} & \xrightarrow{\psi} & G_{n-1} \\ \prod_I \beta_i & \longmapsto & \prod_I \tilde{\psi}(i) \end{array}$$

Let's denote η the embedding of $G_{n-1}, \psi x 1_{G_h}$ (see :VI on page 9) and let's posit: $G \underset{\text{def.}}{=} \eta(G_{n-1-h})$, then:

$$\sum_{G_h}\beta G = \sum_{1+\mathbb{B}_{n-1}}\beta G \qquad \text{and} \qquad \mathscr{A} \underset{\text{def.}}{=} (\beta G)_{1+\mathbb{B}_{n-1}} \text{ is a } P_1\text{-partition of } G_{n-1}$$

Proof:

- the two expressions are equal:

  For $\beta\in G_h$ such that $\beta\in 1+\mathbb{B}_{n-1}$ there's nothing to prove.

  For $\beta\in G_h\setminus\{1+\sigma_1^h\}$, there exists $i\in I_{n-1-h}$ such that $\sigma_i=\beta$, then $\eta(\beta_i x 1_h)=\psi(\beta_i)=\beta_i x\beta$ thus $\beta_i x\beta\in G$, so: $\beta=(\beta_i x 1_h)(\beta_i x\beta)$, with $\beta_i x 1_h\in\mathbb{B}_{n-1}$ and $\beta_i x\beta\in G$

- Since G_n is the direct product of G and G_h (see VI on page 9) , $\mathscr{A}$ is an equipartition.
- Since $\mathscr{A}$ is the orbit of G (G being the stabilizer), for any $\beta, \beta'\in 1+\mathbb{B}_{n-1}$, there exists $\beta"\in 1+\mathbb{B}_{n-1}$ such that $\beta\beta' G=\beta" G$. Now $\forall_{1+\mathbb{B}_{n-1}}\ \beta, \beta' \quad \forall_G\ g \quad d_{n-1}(\beta g, \beta' G)=d_{n-1}(g, \beta" G)=d_{n-1}(\beta", G)\le d_{n-1}(\beta", 1)\le 1$, P_1 holds.

Nota: $G=<\sigma_i\beta_{i+h}>_{[\![1,\,q]\!]}$. Proof: $\pi^q\left(<\sigma_i\beta_{i+h}>_{[\![1,\,q]\!]}\right)=<\beta_{i+h}>_{[\![1,\,q]\!]}\sim G_q$ with $q=n-1-h$ and $G\supset<\sigma_i\beta_{i+h}>_{[\![1,\,q]\!]}$
Back to "Solving the puzzle": chapter XVI on the following page

Now we know from property 1 (see equation 4 on page 20) that $\left((1+\beta_n)\beta G\right)_{1+\mathbb{B}_{n-1}}$ is a P_o-core of G_n.

XIV Existence theorem

Theorem 1:
There exists a P_o-partition of size n of G_n if and only if n is a power of two

Proof:
The condition is sufficient: since we can exhibit such a partition if n is a power of two.(see in chapter XIII on the preceding page)
The condition is necessary: since if we have a P_o-partition of size n in G_n, then it is an equipartition (see XII on page 19), so n divides $|G_n| = 2^n$.Back to "Solving the puzzle": chapter XVI on the following page

XV The prisoners'conundrum

A chessboard with a patchwork of white and black square tiles randomly laid out, possesses one tile under which the key to the prison cell is hidden.
The first prisoner who is shown where the key is, must flip the color of one tile (He turns a black tile into white, or a white one into black) and this is the only piece of information left to his cellmate who, with no more than a look at the chessboard has to devise where the hidden key tile is.
If he guesses correctly, both prisoners are set free.Back to "Abstract": chapter I on page 1

This puzzle has been described here:
3 blue 1 brown puzzle: https://www.3blue1brown.com/lessons/chessboard-puzzle

XVI Solving the puzzle

We number the tiles of the chessboard with $\{1, 2, \cdots, n\} = I_n$ $(n = 64)$ and so a patchwork of black and white tiles is a n-tuples $(a_1, a_2, \cdots, a_n) \in \mathbb{F}_2^n$ where:

$a_i = 0$ if the ith tile is white
$= 1$ otherwise

So basically, what the chessboard displays is a number in $\mathbb{F}_2^n \hookrightarrow \mathbb{N}$ (See chapter II on page 1). And what the first prisoner performs is an action $\beta \in \mathbb{B}_n$, on $\mathbb{F}_2^n \sim G_n$.(See chapter IV on page 3).

If the second prisoner can infer the hidden key tile number from the number he reads on the chessboard this means that he possesses a mapping $\varphi o \varphi_\beta$: $G_n \longrightarrow I_n$, $\beta \in \mathbb{B}_n$, whose images are the hidden key tile numbers, and this is the only way to achieve this, technically we must have (see figure: 5 on the following page):

$$P'_o: \quad \exists \varphi: G_n \supset D \longrightarrow I_n \quad \forall_{G_n} s \quad \forall_{I_n} i \quad \exists_{\mathbb{B}_n} \beta \quad \varphi o \varphi_\beta(s) = i$$

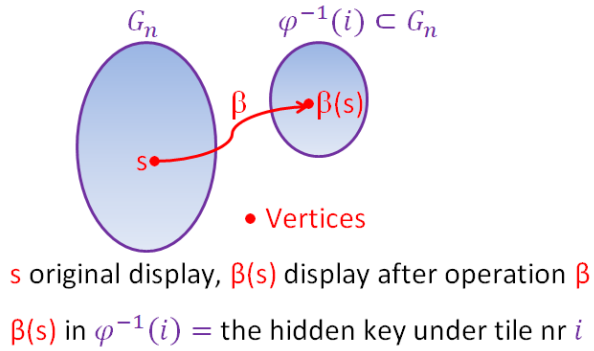
P'_o is equivalent to: There exists a P_o-partition of G_n of size n [60]60:

60
Proof $P'_o \Rightarrow \exists P_o$-partition :

Let's assume we have such a φ in P'_o. $D \subset G_n$ being the domain of φ, necessarily, $\varphi : D \longrightarrow I_n$ is surjective. $\left(\varphi^{-1}(i)\right)_{I_n}$ is a n-set of G_n, and for a given $i \in I_n$ and $s \in G_n$ we can find a β in $\mathbb{B}_n$, such that: $\varphi o \varphi_\beta(s) = i$, thus $\varphi_\beta(s) = \beta s \in \varphi^{-1}(i)$,
with $d_n(s, \beta s) = 1$, so $\left(\varphi^{-1}(i)\right)_{I_n}$ is a P_o-set of size n, and from what precedes (see Remarks in chapter (XII on page 18)) we know it is a P_o-partition (hence $D = G_n$).

Proof $\exists P_o$-partition $\Rightarrow P'_o$:

Figure 5: How to solve?



The puzzle is solvable if and only if we have a P_o-partition of G_n of size n.
And according to theorem 1 in Chapter XIV on the previous page such a partition actually does exist, if and only if n is a power of two, and 64 is:

The puzzle is solvable

XVII Game strategy

Preliminaries

In this chapter, the number of tiles of the chessboard is $n = 2^h$, $n, h \in \mathbb{N}$, the tile number under which the key is hidden will be $key \in [\![0, n-1]\!]$ (the tiles are numbered from 0 to $n-1$), which corresponds to a $\beta_{key} \in G_{n-1}$, the initial display of the last $n-1$ tiles of the chessboard is noted: $board_o \in G_{n-1}$ and can be considered a $(n-1)$-tuple in $\mathbb{F}_2^{n-1}$. A product in G_n is a sum in $\mathbb{F}_2^n$ (see III on page 3), and a product by a β_i for $i = 0, 1, \cdots, n-1$ on $board_o$ would be a flipping of the tile i which corresponds to a sum in $\mathbb{F}_2^{n-1}$, but for $i = 0$ (see action in chapter IV on page 3). We will write a n-tuple from right to left and then simply express it like a number in base 2 (Thus, we will write: $G_4 \ni \beta_1\beta_3 \sim (0, 1, 0, 1)\big[\in \mathbb{F}_2^4\big] \sim 0101 \in \mathbb{N}$, but mind you that the addition in $\mathbb{F}_2^n$ differs from the one in $\mathbb{Z}$, see example III on page 2).

What follows is entirely the result of footnote 59 on page 24 (So refer to it for further details) or footnote 58 on page 23 as a simpler example, so let's have a reminder first:

- We have a partition of size n, in G_{n-1}: the classes of the elements of G_h for the canonical projection π_G, G a subgroup of G_{n-1} isomorphic to G_q (with $q = n-1-h$), namely: $\big(\pi_G(\beta)\big)_{\beta \in G_h}$.

Let $(A_i)_{I_n}$ be a P_o-partition of G_n.
Let be $\varphi = \sum_{I_n} i\chi_i$ where χ_i:

$$\begin{array}{ccll} \bigcup_{I_n} A_i & \xrightarrow{\chi_i} & \{0, 1\} & \\ x & \longmapsto & \chi_i(x) = 1 & \text{if } x \in A_i \\ & & \chi_i(x) = 0 & \text{otherwise} \end{array}$$

φ: $G_n \longrightarrow I_n$, is surjective. For any s in G_n, and i in I_n there exist $s_i \in A_i = \varphi^{-1}(i)$ and $\beta \in \mathbb{B}_n$ such that $\beta s = s_i$, since for A_i, P_o holds, $\varphi(\beta s) = i$, $\varphi o \varphi_\beta(s) = i$. So we posit $D \underset{\text{def.}}{=} G_n$ and we are finished.

- $(\pi_G(\beta))_{\beta\in G_h} = (\pi_G(\beta))_{\beta\in\{1,\,\beta_1,\,\beta_2,\,\cdots,\,\beta_{n-1}\}}$ So that a class of the partition points effectively to a β_i, that is, a chessboard tile i.
- we have an embedding η, such that $\eta_{|G_q} = \psi$ (where ψ is an isomophism from G_q to G), $\eta_{|G_h} = I_d$, with the following commutative diagram (η passes to the quotient):

$$\begin{array}{ccc} G_q \mathrm{x} G_h & \xrightarrow{\eta} & G \mathrm{x} G_h \\ \downarrow{\scriptstyle \pi_h} & & \downarrow{\scriptstyle \pi_G} \\ G_{n-1}/G_q & \xrightarrow{\overline{\eta}} & G_{n-1}/G \end{array}$$

So that the knowledge of η spawns the said partition.[61] 61

The strategy

We read the display of the last $n-1$ tiles (tiles from 1 to $n-1$) as *board* in G_{n-1}, a blank chessboard corresponding to $1 \in G_{n-1}$, or tile 0, and we have a one-to-one correspondence between the tile numbers and the classes of the π_G projection.

Defining: $l \in \{0, 1, 2, \cdots, n-1\}$ by $\pi_G(\beta_l) = \pi_G(board_o.\beta_{key})$ yields: $\pi_G(\beta_{key}) = \pi_G(board_o.\beta_l)$

So, the first prisoner flips the tile l and leaves the $board_o.\beta_l \sim \beta_{key}$ to be read by the second prisoner (Note that $\beta_0 = 1$).

Consequently, the deal for both prisoners is to find the class for π_G of a *board*, a number displayed by the chessboard.

Methodology

First thing to do to get η is to define the injection $(\sigma_i)_{I_q}$ which maps I_q to $G_h \setminus \{1 + \sigma_1^h\}$. Any correspondence table would fit but for big values of n (say $n = 2^{100}$), where you would like to compute it on the fly (And as such alleviates memory load, and data mining), so you could build it like this ($i \in [\![0, n-1]\!]$):

$$\begin{array}{rlll} & \beta_0 & \xrightarrow{\eta} 1 & \sim 0 \\ \text{for: } 1 \le i \le h & \beta_i & \xrightarrow{\eta} \beta_i & \sim 2^{i-1} \\ & \beta_{h+1} & \xrightarrow{\beta_{h+1}\eta} & \sim n-1 \\ \text{for: } h+1 < i \le n-1 & \beta_i & \xrightarrow{\beta_i\eta} & \sim i-h+\mathrm{Min}\left\{k \in \mathbb{N} \text{ such that: } i-h < 2^{k+1}-k\right\}[62] \end{array} \quad 62$$

61

$(\pi_G(\beta))_{G_h} = (\pi_G \mathrm{o} \eta(\beta))_{G_h} = (\overline{\eta} \mathrm{o} \pi_h(\beta))_{G_h} \sim (\pi_h(\beta))_{G_h} \sim (\beta G_q)_{G_h}$

62

Remark:
For any $k \in \mathbb{N}^*$, $2^{k+1} - k > 2^k - (k-1)$ proof: $2^{k+1} - k - 2^k + (k-1) = 2^k - 1$

So this table maps a β_i to $a_i \in G_h$ for $i = 0, \cdots, n-1$ with $\beta_i a_i \in G$, in particular $\pi_G(\beta_i) = \pi_G(a_i)$[63]63

Encoding/Decoding

So we have a $board = board_0.key$ and we want to retrieve the value of l (In order for the first prisoner to flip the tile l), such that: $\pi_G(\beta_l) = \pi_G(board)$.

Let's consider $\pi^q(board) = \prod_I \beta_i$, with $I \subset [\![h+1, n-1]\!]$, for $i \in I$, the conversion table provides us with an $a_i \in G_h$ such that $\eta(\beta_i) = \beta_i a_i \in G$, the same table delivers[64]64 a β_l for an $l \in [\![0, n-1]\!]$ corresponding to $\prod_I a_i \pi_h(board) \in G_h$ then: $\pi_G(\beta_l) = \pi_G(board)$.[65]65

Hereunder an example to see how it actually works.
$h = 4$, $n-1 = 15$, $q = 11$, the conversion table looks like this:

Table of conversion case $n = 16$

i	0	1	2	3	4	5	6	7
$\eta(\beta_i)$	0	**0001**	**0010**	**0100**	1000			
$\beta_i \eta(\beta_i)$						1111	0011	0101

Table of conversion continued

i	8	9	10	11	12	13	14	15
$\beta_i \eta(\beta_i)$	0110	0111	1001	1010	**1011**	1100	1101	1110

63
$\pi_G(\beta_i)\pi_G(a_i) = \pi_G(\beta_i a_i) = 1$

64
Reverse conversion table

for: $0 \leq p \leq h$ $\quad 0 \xrightarrow{\eta^{-1}} \beta_0$, $\quad 2^p \xrightarrow{\eta^{-1}} \beta_{p+1}$, $\quad n-1 \xrightarrow{\eta^{-1}} \beta_{h+1}$

for: $p \in I_{n-2} \setminus \{2^{i-1}\}_{I_{h+1}}$ $\quad p \xrightarrow{\eta^{-1}} \beta_i$ with $i = p + h - \text{Min}\left\{k \in \mathbb{N} \text{ such that: } p < 2^{k+1} - k\right\}$

65
$\pi^q(board) = \prod_I \beta_i, \quad I \subset [\![h+1, n-1]\!], \quad \beta_i \xrightarrow{\text{table}} a_i \in G_h, \quad \eta(\beta_i) = \beta_i a_i \in G$

$\prod_I a_i \pi_h(board) \in G_h \xleftarrow{\text{table}} \beta_l$

$\pi_G(board) = \pi_G(board \prod_I \beta_i a_i)$ since $\prod_I \beta_i a_i \in G$

$= \pi_G(\prod_I a_i \pi_h(board))$ since $board = \pi^q(board)\pi_h(board)$ See notation:VI on page 8

$= \pi_G(\beta_l)$

The first prisoner gets this chessboard in front of him:

0	15	14	13
12	11	10	9
key	7	6	5
4	3	2	1

1. The first prisoner

   - $board_o = \prod_J \beta_i$ with $J = \{2, 4, 5, 7, 10, 12, 15\}$. $key = 8$
   - $\pi^{11}(board_o) = \prod_I \beta_i$ with $I = \{5, 7, 10, 12, 15\}$.
   - $\pi_4(board_o) = \prod_H \beta_i$ with $H = \{2, 4\}$.
   - "+" designates the addition in $\mathbb{F}_2^4$

$$\begin{aligned}
\prod_I \beta_i &\xrightarrow{\text{table}} \prod_I a_i && \sim 1111 + 0101 + 1001 + 1011 + 1110 = 0110 \\
\beta_{key} = \beta_8 &\xrightarrow{\text{table}} a_8 && + 0110 \\
\prod_H \beta_i &\xrightarrow{\text{table}} \prod_H a_i && \sim 0010 + 1000 \quad + 1010 \\
\beta_l = \beta_{11} &\xleftarrow{\text{table}} \prod_{I+H} a_i a_8 && \sim \quad = 1010
\end{aligned}$$

2. The second prisoner inherits this chessboard:

0	15	14	13
12	11	10	9
8	7	6	5
4	3	2	1

   - $board = \prod_J \beta_i$ with $J = \{2, 4, 5, 7, 10, 11, 12, 15\}$.
   - $\pi^{11}(board) = \prod_I \beta_i$ with $I = \{5, 7, 10, 11, 12, 15\}$.
   - $\pi_4(board) = \prod_H \beta_i$ with $H = \{2, 4\}$.

$$\begin{aligned}
\prod_I \beta_i &\xrightarrow{\text{table}} \prod_I a_i \sim 1111 + 0101 + 1001 + 1010 + 1011 + 1110 = 1100 \\
\prod_H \beta_i &\xrightarrow{\text{table}} \prod_H a_i \sim 0010 + 1000 \quad + 1010 \\
\beta_{key} = \beta_8 &\xleftarrow{\text{table}} \quad = 0110
\end{aligned}$$

Here another simpler example, that we could manage on sight:

1	2	3	0
4	*key*	6	7

Thus for the example above, we get:

$h = 3$, $n - 1 = 7$, $board_o \sim 0101010$, $\beta_{key} = \beta_5 \sim 0010000 = 2^4$, $\beta_0 \sim 0$

This delivers the following table:

$$\text{for: } 1 \le i \le 3 \qquad \beta_i \xrightarrow{\eta} \beta_i \sim 2^{i-1}$$

$$\beta_4 \xrightarrow{\beta_4\eta} \sim 7 = 111$$

$$\beta_5 \xrightarrow{\beta_5\eta} \sim 3 = 011$$

$$\beta_6 \xrightarrow{\beta_6\eta} \sim 5 = 101$$

$$\beta_7 \xrightarrow{\beta_7\eta} \sim 6 = 110$$

However for so simple an example, in order to decipher swiftly at a glance at the chessboard, we'd rather have the more suitable following conversion table :

Table of conversion case $n = 8$

i	0	1	2	3	4	5	6	7
$\eta(\beta_i)$	0	001	010	100				
$\beta_i\eta(\beta_i)$					110	101	011	111

Now hereunder a procedure (which actually performs the expected calculations) to get the tile numbers from this example:

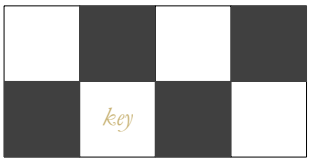
The first prisoner procedure:

1. Count the black tiles in the bottom row, add 1 if the key is in bottom row, you get n
2. Add the upper and the bottom rows of the first 3 columns of the chessboard, the sum is a three digit r (the black tiles stand for unit digits, the white tiles for 0).
3. Add 1 to the rank of r which corresponds to the column where the key is (Thus if the key is in the last column you add nothing), the result is s.
4. If n retrieved at the first step is odd add 111 to s, you get the final result.
    - If the result is 111, the tile to flip is the bottom right one.
    - If the result is 000, the tile to flip is the top right one.
    - If the result contains two unit digits, the tile we look for flipping is in the first 3 columns in the bottom row designated by the location of the zero digit in the result.
    - If the result contains one unit digit, the tile to flip is the one in the first 3 columns in the upper row designated by the location of the unit digit in the result.

The second prisoner procedure:

1. Get the number n of black tiles in the bottom row.
2. Add the upper and the bottom rows of the first 3 columns of the chessboard, the sum is a three digit r.
3. If n retrieved at the first step is odd add 111 to r, you get the result.
    - If the result is 111, the hidden key tile is the bottom right one.
    - If the result is 000, the hidden key tile is the top right one.
    - If the result contains two unit digits, the hidden key tile we look for is in the first 3 columns in the bottom row designated by the location of the zero digit in the result.
    - If the result contains one unit digit, the hidden key tile we look for is in the first 3 columns in the upper row designated by the location of the unit digit in the result.

Application



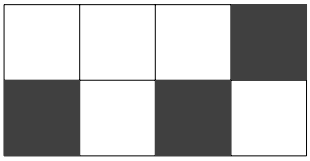
The chessboard displays: 0101
1010 , with *key* = **0100**, bottom row.

The first prisoner does:

1. The number of black tiles in the bottom row is 2 added up to 1, because the key is in the bottom row, gives 3.
2. The first three digits of the bottom row: 101 and the first three digits of upper row: 010 add up to: 101+010=111.
3. The key is in the second column (commencing left hand side), we add 1 to the previous result at rank 2, we get: 111+010=101.
4. The parity retrieved at the first step is odd, so we add 111, we get: 101+111=010.

    - The result contains one unit digit, the tile we look for is in the first 3 columns of the upper row designated by the location of the unit digit in **010**, this is the 2sd tile.
    - the prisoner flips the second from left upper row tile.

The second prisoner is then facing to the chessboard:



The chessboard displays: 0001
1010

The second prisoner does:

1. The number of black tiles in the bottom row is 2, thus even.
2. The first 3 column upper row and the first 3 column bottom row add up to: 000+101=101.
3. (The parity retrieved at the first step is even.)

    - The result: 101 contains two unit digits, the tile we look for is in the bottom row designated by the location of the zero digit in **101**, thus the sought tile is the second from left in bottom row.

So now with little training you might be able to code and decode at a glance (At least for the 8 tile chessboard).

The end